WHAT IS CLAIMED IS:

1. A modular multiplication device for implementing an information encryption/decryption technique in which message (A) is encrypted/decrypted using a first key (B) and a second key (N), comprising:

a storage device for storing the message, the first key, and the second key, each being n bits in length;

a recording logic for generating at each clock a first n+4bit signal using the message and the first key;

a first carry save adder for generating a 3bit sequence consisting of one carry value and two sum values using the first n+4bit signal and two parallel n+4bit input signals;

a quotient logic for generating a 3bit determiner for determining a modular reduction multiple using the 3bit sequence and one carry value;

a selector for generating a second n+4bit signal using the second key and the 3bit determiner;

a second carry save adder for generating a pair of sum values and a pair of carry values using the second n+4-bit signal, and respective sum and carry terms outputted from the first carry adder; and

a first full adder for generating a carry input value by performing a full addition operation with the pair of sum and carry values and a ~~preset circuitry~~ carry value (cin) outputted from the quotient logic at a previous clock.

2. The device of claim 1, wherein the storage device contains shift registers for storing the respective message, first key, and second key.

3. The device of claim 1, wherein the message is right-shifted by 2 bit positions at every clock.

4. The device of claim 1, wherein the first n+4bit signal is one of 0, B, 2B, -B, and –2B.

5. The device of claim 1, wherein the second n+4bit signal is one of 0, N, 2N, -N, and -2N.

6. The device of claim 1, wherein the recording logic comprises:

a booth recording circuit for performing booth recoding with the two least significant bits of the message;

a multiplexer for multiplexing the two least significant bits and the first key, and outputting one of 0, B, and 2B; and

a one's complementary operator for performing a one's complementary operation on the n+1bit signal outputted from the multiplexer according to the two least significant bits and generating one of 0, B, 2B, -B, and –2B.

7. The device of claim 1, wherein the first carry save adder comprises n+4 second full adders, each performing a full addition operation with corresponding sum and carry bits of the two parallel n+4 input signals and corresponding bit of the first n+4bit signal, and producing the 3bit sequences.

8. The device of claim 7, wherein a first one of the two parallel n+4 bit input signals is created by selecting the most significant n+2 bits from a sum term of the

second carry save adder and inserting 2 bits as the most significant bits of the selected n+2 bits.

9. The device of claim 8, wherein the two most significant bits are zeros.

10. The device of claim 8, wherein a second one of the two parallel n+4 bit input signals is created by selecting the most significant n+3 bits from a carry term of the second carry save adder and inserting one bit as the most significant bit of the selected n+3 bits.

11. The device of claim 10, wherein the one most significant bit is zero.

12. The device of claim 1, wherein the quotient logic comprises:

a D flip-flop for temporally storing the carry input value from the first full adder;

a third full adder for performing a full addition operation on the carry input value, a sum value outputted from a least significant full adder of the first carry save adder, and a sign bit of the first n+4bit signal ~~in~~;

an exclusive OR (XOR) logic gate for performing an exclusive OR operation on the carry value outputted from the least significant full adder of the first carry save adder, a sum value outputted from a secondly least significant full adder of the first carry save adder, and the carry value of the third full adder; and

a combinational circuit for combining the outputs of the third full adder , exclusive OR logic gate and a second least significant bit of the second key, and outputting the 3bit determiner signal.

13. The device of claim 1, wherein the second carry save adder comprises n+4 fourth full adders, each performing a full addition operation with corresponding sum and carry bits from the first carry save adder except for a least significant sum bit and a most significant carry bit and a corresponding bit of the second n+4bit signal, and producing the pairs of sum and carry values.

14. The device of claim 1, wherein the first full adder performs a full addition with a sum value output from a second least significant full adder of the second carry save adder, a carry value outputted from a least significant full adder of the second carry save adder, and a carry value (cin) outputted from the quotient logic at a previous clock, and produces the carry input value.

15. The device of claim 1 further comprising a carry propagation adder for performing a carry propagation addition operation with the sum and carry terms outputted from the second carry save adder after m+2 clock, where m=n/2.

16. The device of claim 15, wherein the carry propagation adder adds modulus second key to a result of the carry propagation addition operation if an output of the carry propagation adder is negative value.

17. A modular multiplication device for implementing a message encryption/decryption technique in which the message (A) is encrypted/decrypted using a first key (B) and a second key (N), comprising:

a storage device for storing the message, the first key, and the second key, each of n bits in length;

a recording logic for generating at each clock a first n+3bit signal using the

message and first key;

a first carry save adder for outputting a 3bit sequence consisting of one carry value and two sum values by performing a first carry save addition operation with the first n+3bit signal and two parallel n+3bit input signals;

a quotient logic for generating a 2bit determiner for determining a modular reduction multiple by performing a quotient operation with the 3bit sequence and the one carry value;

a selector for generating a second n+3bit signal using the second key and the 2-bit determiner;

a second carry save adder for outputting a pair of sum values and a pair of carry values by performing a second carry save addition operation with the second n+3-bit signal, and respective sum and carry terms outputted from the first carry addition operation;

an AND logic gate for outputting a carry input value by performing an AND operation with the pair of sum and carry values.

18. The device of claim 17, wherein the storage device contains shift registers for storing the respective message, first key, and second key.

19. The device of claim 18, wherein the message is shifted by 2 positions at every clock.

20. The device of claim 17, wherein the first n+3bit signal is one of 0, B, 2B, and 3B.

21. The device of claim 17, wherein the second n+3bit signal is one of 0, N,

2N, and 3N.

22. The device of claim 17, wherein the recording logic is a multiplexer which multiplexes two least significant bits of the message and n bits of first key, and outputs the first n+3 bit signal.

23. The device of claim 12, wherein the first carry save adder comprises n+3 first full adders, each performing a full addition operation with corresponding sum and carry bits of the two parallel n+3bit input signals and a corresponding bit of the first n+3bit signal, and outputting the 3bit sequence.

24. The device of claim 23, wherein a first one of the two parallel n+3bit input signals is created by selecting the most significant n+1 bits from a sum term of the second carry save adder and inserting two bits as the most significant bits of the selected n+1 bits.

25. The device of claim 24, wherein the two most significant bits are zeros.

26. The device of claim 24, wherein a second one of the two parallel n+3bit input signals is created by selecting the most significant n+2 bits from a carry term of the second carry save adder and inserting 1 bit as the most significant bit of the selected n+2 bits.

27. The device of claim 26, wherein the one most significant bit is zero.

28. The device of claim 17, wherein the quotient logic comprises:

a D flip-flop for temporally storing the carry input value from the AND logic gate;

a half adder for performing a half addition operation with the carry input value and a sum value output from a most significant fuller adder of the first carry save adder;

an exclusive OR (XOR) logic gate for performing an exclusive OR operation with a carry value output from the least significant full adder of the first carry save adder, a sum value output from a second least significant full adder, and an output of the half adder;

a combinational circuit for combining the outputs of the half adder and the exclusive OR logic gate and a second least significant bit (n1) of the second key and outputting the 2bit determiner signal.

29. The device of claim 17, wherein the second carry save adder comprises:

n+3 second full adders, each performing a full addition operation with corresponding sum and carry bits from the first carry saver adder, except for a least significant sum bit and the most significant carry bit, and a corresponding bit of the second n+3bit signal , and producing the pairs of sum and carry bits.

30. The device of claim 17, wherein the AND logic gate performs an AND operation with a sum value output from a second least significant second full adder of the second carry save adder and a carry value output from a least significant second full adder of the second carry save adder , and produces the carry input value.

31. The device of claim 17 further comprising a carry propagation adder for performing carry propagation addition operation with the sum and carry terms output

from the second carry save adder after m+2 clock, where m=n/2.

32. A modular multiplication method for implementing a message encryption/decryption technique in which a message (A) is encrypted/decrypted using a first key (B) and a second key (N), comprising:

storing the message, first key, and second key each of n bits ;

generating a first n+4bit signal using the message and first key at each clock;

outputting a 3bit sequence consisting of one carry value and two sum values by performing a first carry save addition operation with the first n+4bit signal and two parallel n+4-bit input signals;

generating a 3-bit determiner for determining a modular reduction multiple by performing a quotient operation with the 3bit sequence and one input carry value;

generating a second n+4bit signal using the second key and the 3bit determiner;

outputting a pair of sum values and a pair of carry values by performing a second carry save addition operation with the second n+4bit signal, and respective sum and carry terms output from the first carry save addition operation;

outputting a carry input value by performing a full addition operation with the pair of sum and carry values and a carry value outputted from the quotient logic at a previous clock.

33. The method of claim 32, wherein the message is right-shifted by 2 bits at every clock.

34. The method of claim 32, wherein generating the first n+4bit signal includes:

performing booth recording with the two least significant bits of the message; and

generating, one of 0, B, 2B, -B, and -2B according to the two least significant bits.

35. The method of claim 32, wherein a first one of the two parallel n+4- bit input signals is created by selecting the most significant n+2 bits from a sum term outputted by the second carry save addition operation and inserting 2 bits as the most significant bits of the selected n+2 bits.

36. The method of claim 32, wherein the two most significant bits are zeros.

37. The method of claim 32, wherein a second one of the two parallel n+4 input signals is created by selecting the most significant n+3 bits from a carry term of the second carry save addition operation and inserting one bit as the most significant bit of the selected n+3 bits.

38. The method of claim 32, wherein the one most significant bit is zero.

39. The method of claim 32, wherein the 3bit sequence includes two sum values and one carry value.

40. The method of claim 39, wherein the two sum values are a least significant bit and a second least significant bit of a sum term output from the first carry save addition operation.

41. The method of claim 39, wherein the one carry value is a least significant bit of a carry term output from the first carry save addition operation.

42. The method of claim 32, wherein the one input carry value is the carry input value generated by the full addition operation.

43. The method of claim 32, wherein the second n+4bit signal is selected from among 0, N, -N, and -2N according to the two least significant bits of the 3bit determiner.

44. The method of claim 32, wherein the pair of sum and carry values are a second least significant bit of a sum term and a least significant bit of the carry term outputted from the second carry save addition operation.

45. The method of claim 32, wherein the most significant bits of the sum and carry terms outputted from the first carry save addition operation are ignored.

46. The method of claim 32, further comprising performing a carry propagation addition operation with the sum and carry terms after m+2 clock, where m=n/2.

47. The method of claim 46, further comprising adding a modulus second key if an output of the carry propagation addition operation is a negative value.

48. A modular multiplication method for implementing a message encryption/decryption technique in which message (A) is encrypted/decrypted using a

first key (B) and a second key (N), comprising:

storing the message, first key, and second key, each of n bits in length;

generating a first n+3bit signal using the message and first key at each clock;

outputting a 3bit sequence consisting of one carry value and two sum values by performing a first carry save addition operation with the first n+3bit signal and two parallel n+3bit input signals;

generating a 2bit determiner for determining a modular reduction multiple by performing a quotient operation with the 3bit sequence and one input carry value;

generating a second n+3bit signal using the second key and the 2bit determiner;

outputting a pair of sum values and a pair of carry values by performing a second carry save addition operation with the second n+3bit signal, and respective sum and carry terms outputted from the first carry addition operation;

outputting a carry input value by performing an AND operation with the pair of sum and carry values.

49. The method of claim 48, wherein the message is right-shifted by 2 bits at every clock.

50. The method of claim 48, wherein the first n+3 bit signal is produced by multiplexing the two least significant bits of the message and the first key.

51. The method of claim 48, wherein the first n+3bit signal is one of 0, B, 2B, and 3B.

52. The method of claim 48, wherein a first one of the two parallel n+3bit

input signals is created by selecting the most significant n+1 bits from a sum term of the second carry save addition operation and inserting two bits as the most significant bits of the selected n+1 bits.

53. The method of claim 52, wherein the two most significant bits are zeros.

54. The method of claim 52, wherein a second one of the two parallel n+3bit input signals is created by selecting the most significant n+2 bits from a carry term of the second carry save addition operation and inserting 1 bit as the most significant bit of the selected n+2 bits.

55. The method of claim 54, wherein the one most significant bit is zero.

56. The method of claim 48, wherein the 3bit sequence includes two sum values and one carry value.

57. The method of claim 56, wherein the two sum values are a least significant bit and a second least significant bit of a sum term output from the first carry save addition operation.

58. The method of claim 56, wherein the one carry value is a least significant bit of a carry term output from the first carry save addition operation.

59. The method of claim 48, wherein the one input carry value is the carry input value generated by the AND operation.

60. The method of claim 48, wherein the second n+3bit signal is selected from among 0, N, 2N, and 3N according to 2-bit determiner.

61. The method of claim 48, wherein the pair of sum and carry values are a second least significant bit of a sum term and a least significant bit of the carry term output from the second carry save addition operation.

62. The method of claim 48, wherein the most significant bits of the sum and carry terms output from the first carry save addition operation are ignored.

63. The method of claim 48, further comprising performing a carry propagation addition operation with sum and carry terms output from the second carry save addition operation after m+2 clock, where m=n/2.